Paris, April 2024

Artificial Intelligence Working Group Position Paper
Key messages on the AI Act Proposal

Paris Europlace is the organization in charge of promoting and developing the Paris financial center. We are a privileged intermediary of European and French authorities, with which we maintain a continuous and constructive dialogue. Our aim is to promote financial markets to international investors, issuers and financial intermediaries to better finance the real economy and the energy transition. Paris Europlace gathers more than 600 members, including investors, sustainable finance entities, banks, financial market authorities, corporates, consulting firms.

Artificial Intelligence (AI) represents a major technological advancement aiming to mimic human cognitive processes through machines and computer systems. These systems utilize algorithms and statistical models to analyze data, identify patterns, and make predictions. AI can be classified into three main categories:

1. Narrow AI (ANI): tailored for specific tasks like language translation, image recognition, or speech recognition, ANI excels within its domain but lacks versatility.
2. General AI (AGI): aims to mirror human cognitive abilities such as learning, problem-solving, and decision-making. AGI's potential to transform many areas is tempered by concerns about its impact on society and employment. Yet, we are still far away from having AI that is capable of performing as well as (or better than) humans on a wide range of cognitive tasks.
3. Super AI (ASI): theoretical advance AI that could surpass human capabilities in any field. The development of ASI, would it be fully operational, could give rise to considerable technical, ethical and safety issues, and its potential is not yet fully understood.

Moreover, the digital transformation, facilitated by the rapid evolution of AI, has created significant opportunities. Specifically, Generative Artificial Intelligence, often referred to as "Generative AI", has been identified as a fast-evolving area with a potentially major impact on businesses. Generative AI is a subset of AI that focuses on the autonomous creation of new content, such as texts, images or videos, through computer systems.

At the European level, considerable efforts have been made to capitalize on these opportunities and create a common legislative framework for responsible AI. The EU has been working on regulating on AI since 2020, with its first Position Paper on AI. In 2021, the European Commission made its proposal for the first EU framework for regulating AI, the AI

Act, which has been intensively negotiated until this March. It was indeed essential to reach an agreement before the next European elections in June, to avoid jeopardizing this long-term project and undermining European sovereign autonomy. The AI Act was finally approved by the Member States in February 2024. On March 13th, 2024, the European Parliament plenary vote approved the legislation on AI.

The AI Act aims at regulating the use of artificial intelligence by adopting a risk-based approach. Its primary objective is to promote the development of trustworthy and innovative AI while ensuring respect for fundamental rights and European values. AI systems will be categorized based on risks, with reinforced obligations for high-risk systems and less extensive obligations for those posing limited risks.

The different types of AI systems include:

- Prohibited AI systems: certain uses of AI, such as behavior manipulation or real-time biometric systems in public spaces for law enforcement purposes, will be prohibited.
- High-risk AI systems: companies will be subject to various obligations related to documentation, risk management systems, governance, transparency or security, depending on their classification. These systems will have to be declared to the EU and bear a CE marking.
- AI systems presenting specific risks and General Purpose AI models (GPAI): an obligation of information will be imposed for systems interacting with humans (e.g. chatbots) or generating/manipulating content such as "deep fakes". Specific requirements will apply to GPAI models, especially those which could pose “systemic risks”.
- Low-risk AI systems: encouragement for the voluntary creation of codes of conduct for these systems like spam filters or video games.

From a liability perspective, the AI Act categorizes organizations into seven categories based on their role in the chain and assigns appropriate responsibilities: provider, importer, distributor, deployer (the using company), operator, manufacturer, and affected person. The aim of the AI Act is to address the entire chain, although the particular focus is on providers and deployers of high-risk AI systems. Providers of these systems will have to comply with the Act's requirements regarding risk assessment, data governance (including bias mitigation), technical documentation, record-keeping, transparency, human oversight, robustness and cybersecurity in their development processes, on top of other obligations such as implementing quality management systems, registering the AI systems to an EU database and affixing CE marking. Deployers will be held responsible for using these high-risk AI systems in accordance with the instructions of use accompanying the systems, for example by implementing human oversight.

The regulation is overseen by the European AI Office, and national authorities will ensure compliance with the requirements of the AI Act, including registration in a European database

and obtaining CE certification for high-risk AI before market placement. In France, discussions continue over which authority will oversee AI Act compliance. The CNIL's creation of an AI Committee suggests its potential involvement, but other French institutions may also play a role. The CNIL and its counterparts indicated that, as they were already in charge of implementing the GDPR and had extensive practical and theoretical knowledge of the legislation applicable to data protection, they could draw on their experience to implement governance that was as harmonized as possible.

But several points of concern arise:

- Firstly, there could be an information asymmetry between deployers and providers, especially when deployers become providers, potentially leading to compliance gaps or inconsistencies.
- Secondly, there is a latency issue in notifying authorities about high-risk AI systems' deployment, as providers must await responses, potentially requiring authorization rather than mere notification. Additionally, the fluidity in defining high-risk AI categories poses challenges for both providers and users in anticipating future additions to the list.
- Furthermore, conducting Fundamental Rights Impact Assessments (FRIA) before deployment demands full cooperation from providers, incurring additional costs and time. The uncertainty surrounding which systems might be classified as high-risk in the future poses difficulties for planning and compliance efforts for both providers and users. Despite these points of concerns, the AI Act adoption marks a significant step towards responsible and ethical use of AI in the EU.

However, some French companies expressed reservations, particularly concerning the regulation of Generative AI models. In addition, French authorities sought to adapt certain provisions of the text, especially regarding the confidentiality of training data and the qualification of "systemic" models subject to reinforced risk management obligations. The aim was to give companies greater room for maneuver, so that they could compete on a level playing field with other jurisdictions.

Paris Europlace fully supports the objective of facilitating the competitiveness of EU-based entities, with subsidiarity and proportionality to be properly respected by the EU regulation. During the future reviews of the text, Paris Europlace will pay attention to also ensure that regulation continues to evolve in line with technological advancements. Indeed, an additional complexity for private firms is to rapidly adjust their current frameworks to integrate AI governance or to create a governance structure from scratch.

In addition, the regulation also aims to boost the development of AI within the EU to compete with non-EU giants. As for testing AI before market launch or deployment, the AI Act mandates each national authority to establish a regulatory sandbox. These sandboxes will enable companies to test AI systems, thus promoting innovation. Real-world testing is also made

possible if experiments can be conducted by AI providers with consent from users and relevant national authorities, under specified conditions of security, transparency and supervision. These test environments should be under the control of a national authority, which may be the CNIL in France, although other domestic authorities (e.g. ACPR or ANSSI) could be involved in supervising regulatory provisions. This point thus raises questions about the extent of the powers of national authorities: for example, the CNIL initially only covers personal data; while AI systems can pose risks even if they do not process personal data. Consequently, the new complexity of complying with this regulation raises significant concerns, particularly regarding governance, IT costs and regulatory burden.

All in all, as there is no one-size-fits-all organizational structure for AI governance, private companies need to plan and identify the AI governance structure that best fits their organizational structure be it centralized, decentralized or hybrid. Organizations need to identify the leadership council, a support for AI initiatives, as well as specific roles and responsibilities at the strategic and operational levels. Therefore, Paris Europlace Working Group on AI recommends the establishment of three essential governance pillars:

1. Defined roles and responsibilities: in particular, barring justified exceptions (e.g. mutualization within a group or a subgroup of companies within a firm), considering the appointment of a cross-functional leader, with some independence in its risk assessment approach, empowered to monitor information on all AI-related aspects of the firm. Involvement of key stakeholders in the processes is needed for a comprehensive approach.
2. Operational and strategic committee: management committees should define guidelines for responsible AI, especially to make decisions related to the bias/performance balance. It is also recommended to participate in already existing committees to avoid multiplying instances and increasing the teams' workload, especially those established for personal data protection.
3. Structured and sustainable processes: mapping AI systems, integrating risk management from the project phase, and considering risks in daily activities are essential steps. Risks associated with AI fall into two distinct categories: ethical risks and operational risks, both of which also intersect with ESG factors.

On the one hand, ethical risks encompass various concerns such as the absence of human action and loss of human control, damage to the systems' security and reliability, privacy violations, lack of transparency and adverse social impacts. Additionally, the lack of inclusion and diversity in the development and deployment of AI systems can exacerbate social issues such as algorithmic bias, discrimination and social inequalities.

On the other hand, operational risks include aspects such as third-party and system failures, internal and external fraud, compliance with product and regulatory requirements, damage to physical assets, execution and process failures, financial and reporting failures, as well as project management failures. Moreover, these risks can align with ESG factors across various

dimensions, including energy consumption, data privacy, security, supply chain management, stakeholder relations, and ESG regulations (e.g. CSRD).

The potential origin of these risks can be attributed to various factors, such as the source data used by AI models (personal data, open data, IoT), the underlying algorithm of the AI model, the use case defining the model's objective, but also the lack of human oversight. Therefore, a proactive management of these risks is important to ensure responsible and ethical use of AI, while minimizing negative impacts on operations and society. This necessitates the implementation of processes for data quality, transparency, documentation and risk management, during both system development and deployment.

It is essential to begin the journey of responsible AI by mapping existing and future systems to assess the level of risk and, consequently, the level of exposure to regulatory obligations. The goal is then to build a responsible AI strategy and define its governance as presented above. The central pillar of all this remains training and change management at all levels: top management, managers, operational staff, etc. In other cases, leaders cannot make informed decisions regarding the use of AI and its impact on the business. Upskilling will help avoid or mitigate issues related to bias intellectual property, trade secrets, as well as data protection.

*

In conclusion, the Paris Europlace Working Group on AI recognizes the opportunities offered by AI, especially generative AI, but emphasizes the need for a proactive governance to ensure not only compliance with AI regulations but also adequate risk management practices, especially for some AI systems which may not be subject to specific AI regulatory measures.

Consequently, given the changes to be made in their internal governance and risk management processes, and to facilitate the preparation by banking, financial and insurance players of the implementation of the AI Act, it is of the utmost importance to clarify certain key concepts of the AI Act for these industries.

- The need for clarification may be cross-sectorial, for example regarding the need of clear criteria to identify precisely AI systems and GPAI subject to the AI Act.
- It may be also specific to the banking, financial and insurance sectors, for example: (i) the categorization of certain systems used in these industries as AI systems or GPAI pursuant to the AI Act and (ii) the categorization of the regulated entities according to the classification provided in the AI Act (providers, deployers, etc.).

For this purpose, it is urgent to obtain more visibility on the authority or authorities which will be competent for the supervision of the AI Act, including with regards to the banking, financial and insurance players. In the future supervisory framework, a leading role should be organized

for the sectorial regulators, which have the in-depth understanding of the sectorial stakes and will be best placed to provide the necessary sectorial guidance.

Furthermore, the AI Act requires the creation of regulatory sandboxes, which can help market players to develop the appropriate setup to comply with the new regulation. The designation of the national competent authorities in France is also crucial for defining as soon as possible the conditions in which the AI regulatory sandbox will be put in place and operated in France and the extent to which it could benefit to banking, financial and insurance players to prepare for the AI Act.

Last, the Working Group underlines some concerns about European funding and sovereignty, particularly the risk of promising AI companies being acquired by foreign investors. Preserving technological sovereignty and fostering national talents are essential to maintaining Europe's competitiveness and open autonomy in the AI sector.